UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/765,108	01/16/2001	Alexander Medvinsky	018926006400	8249

20350 7590 04/22/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/765,108	MEDVINSKY, ALEXANDER	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 10-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 10-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 January 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/18/2005, applicant amends claims 1, 6, 13, 17, and 19; cancels claims 8 and 9. The following claims 1-7 and 10-23 are presented for examination.

1.1 In response to communications filed on 1/18/2005, the USC 101 rejection to claims 11-12, 15-16, and 21-22 has been withdrawn.

1.2 Applicant's arguments, pages 9-11, filed on 1/18/2005, with respect to the rejection of claims 1-23 have been fully considered but they are not persuasive. Independent claims 1, 6, 13, 17, and 19 have been amended to include the limitations "having a timestamp synchronization source operable to synchronize cryptographic operations between said local multimedia adapter and said remote multimedia terminal adapter". Applicant states that Klinger does not disclose a timestamp as synchronization. Examiner respectfully disagrees. Klinger discloses in one embodiment sending messages that include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the

recitation of a timestamp as a synchronization source to synchronize cryptographic operations. Applicant discloses on page 8, lines 27-30, and "a 'time stamp' is any mechanism for performing synchronization for a cipher to attain decryption of encrypted data." Dent and Crichton also disclose timestamp for synchronization of cryptographic operations. Applicant also requested that the portions of the provisional application to Klinger reference be cited. The scope of the invention of Klinger is disclosed in the provisional application and some of the details are not present as they are known in the art; in addition some related patents are disclosed in the provisional reference and combining the references would have been obvious to one skilled in the art, consequently the claims are now rejected under 35 USC 103(a). Applicant has not overcome the rejection by amending the claims. Therefore, claims 1-7 and 10-23 remain rejected in view of the same references. Other claims not challenged by the applicant still apply in this Office Action.

Claim Objections

2. Claims 1, 6, 13, 17, and 19 are objected to for lack of indentation of limitation. See MPEP § 608.01(m). Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 11, 12, 15, 16, 18, 21, and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 11, 12, 15, 16, 18, 21, and 22, the phrase "for example" renders the claim indefinite because it is unclear whether the limitation gateway controller following the phrase is part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 1-3, 6-7, 10-16, and 19-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al** in view of US Patent 5,081,679 to **Dent**.

4.2 **As per claims 1 and 19, Klingler et al.** discloses a system for securely transmitting Real Time Protocol voice packets during a communication session with a remote multimedia terminal adapter over an Internet protocol network; the system comprising: Klinger discloses in one embodiment a system comprising remote units and base stations for sending/receiving messages, messages include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the recitation of a local multimedia terminal adapter receiving the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter, the local multimedia terminal adapter comprising, a local key stream generator for generating a first key stream, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); a packet encryptor that encrypts the voice packets using at least a portion of the first key stream to form encrypted voice packets, forwarding the encrypted voice packets from the local location to the remote location for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); the remote multimedia terminal adapter receiving the encrypted voice packets, the remote multimedia terminal adapters further comprising, a remote key stream generator for generating the first key stream in order to decrypt the encrypted voice packets, for example (see page 3, paragraphs 0039-0041; page 2, paragraphs 0027, 0032, 0033); and a packet decryptor decrypting the encrypted voice packets using the first key stream, for example (see page 3, paragraphs 0039-

0041; page 2, paragraphs 0027, 0032, 0033), wherein both key stream generators are capable of generating a second key stream to prevent reuse of any portion of the first key stream during the communication session, for example (see page 8, paragraph 0101). **Dent** in an analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time and counters because it is important for the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51).

As per claims 2 and 20, Klingler et al. discloses the limitation of wherein the second key stream is generated when the system wishes to switch from a first to a second coder/decoder for compression/decompression of the voice packets, for example (see page 8, paragraphs 0100-0101 and page 10, claims 18-21).

As per claim 3, **Klingler et al.** discloses the limitation of wherein the second key stream is generated when a Message Authentication Code algorithm change occurs, for example (see page 6, paragraphs 0086-0089; pages 1-2, paragraph 0026 and page 10, claims 18-21).

As per claim 6, **Klingler et al.** discloses a system for communicating Real Time Protocol voice packets between a local and a remote location over an Internet protocol network, the system comprising: a stream cipher module for encrypting the voice packets, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); and a key stream generator for generating a first Real Time Protocol key stream, the stream cipher module employing the first key stream to encrypt the voice packets for forwarding to the remote location, the key stream generator producing a second Real Time Protocol key stream for encrypting the voice packets when the system wishes to switch from a first communication parameter to a second communication parameter, each of the first and second parameters being involved in the synchronization of the key stream, for example (see pages 6-7, paragraphs 0086-0090; page 8, paragraphs 0101-0103 and page 10, claims 18-21, 33 and abstract). Klinger discloses voice messages that include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the recitation of wherein the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote

multimedia terminal adapter. **Dent** in an analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time and counters because it is important for the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51).

As per claim 7, Klingler et al. discloses the limitation of wherein the first communication parameter is a first coder/decoder that compresses/decompresses the voice packets, and the second communication parameter is a second coder/decoder that compresses/decompresses the voice packets, for example (see page 2, paragraph 0032).

As per claim 10, **Klingler et al.** discloses the limitation of further comprising a new time stamp sequence generated when the second Real Time Protocol key stream is generated, for example (see page 7, paragraphs 0093-0094).

As per claim 23, **Klingler et al.** discloses the limitation of further comprising a synchronization source for synchronizing and enabling decryption of the voice packets at the remote location, for example (see pages 1-2, paragraph 0026).

As per claim 13, **Klingler et al.** discloses a method for securely transmitting Real Time Protocol voice packets from a local to a remote location via a communication network, the method comprising: generating a first Real Time Protocol key stream for encrypting the voice packets; forwarding encrypted voice packets to the remote location, for example (see page 3, paragraphs 0038-0041 and page 7, paragraphs 0093-0094); generating a second Real Time Protocol key stream for encrypting the voice packets in response to a request to change communication parameters for the same media stream, for example (see pages 6-7, paragraphs 0086-0094; page 8, paragraphs 0101-0103 and page 10, claims 18-21, 33 and abstract); and forwarding voice packets encrypted with the second Real Time Protocol key stream to the remote location, for example (see page 8, paragraphs 0101-0103). Klinger discloses voice messages that include control data and payload data wherein the control data contains a particular control message used to initiate an encryption synchronization process including triggering a synchronization counter with a size of a message that allows determining when the last block of the message has been transmitted as the counter decrements to zero then initializing

the cryptosystem (page 9, claims 8-10 and pages 1-2, paragraph 0026) that meets the recitation of wherein the voice packets having a timestamp as a synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter. **Dent** in an analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). **Dent** also discloses using real-time and counters because it is important for the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide timestamp synchronization source to synchronize cryptographic operations between said local multimedia terminal adapter and said remote multimedia terminal adapter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Dent** so as to enable the receiver to be operated in synchronism with the transmitter keystream generator for the message to be properly decoded (column 12, lines 23-51).

As per claim 14, Klingler et al. discloses the limitation of further comprising reinitializing a time stamp for synchronizing decryption of the voice packets, for example (see pages 1-2, paragraph 0026).

As per claims 11, 15, and 21, Klingler et al. discloses the limitation of providing key derivation or a pseudorandom function based on a counter, and shared secret key, for example (see page 7, paragraph 0089, 0094; page 8, paragraphs 0101-0105) that meets the recitation of wherein the second key stream is generated by re-executing the following key derivation function: F(S, "End-End RTP Key Change <N>") where N is a counter incremented whenever a new set of Real Time Protocol keys is re-derived for the same media stream session; F( ) is a one-way pseudo-random function used for the purpose of key derivation; S is a shared secret - a random value shared between the two endpoints and is known only to those two endpoints and possibly a trusted server (e.g. gateway controller); and "End-End RTP Key Change <N>" is a label that is used as a parameter to the key derivation function F(), <N> stands for an ASCII representation of a decimal number, representing a counter. **Klingler et al.** discloses the same result and also discloses algorithm for key generation in pages 4-5. Similar algorithm in the claimed invention of f as a function of a secret key and a parameter can be found in cryptography textbook known in the art, which does not depart from the spirit and scope of the invention disclosed by **Klingler et al**. **Dent** in an analogous art teaches a system for bit synchronization using a timeout parameter a handoff counter as a basis to generate new key and further discloses changing the parameter to fit individual circumstances, for example (see column 15, lines 20-50). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and system of **Klingler et al** to provide a key generation as a function of a secret key and a counter as taught by **Dent**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Dent** so as to selectively change the parameter to fit individual circumstances.

Claims 12, 16, and 22 are similar to the rejected **claims 11, 15, and 21** except for adding a source identifier, which is known in the art as found in US patents 6,2754,71 and 6,122,665. **Klingler et al.** also uses an identifier to identify the source of the message, for example (see page 2, paragraph 0032). Therefore, **claims 12, 16, and 22** are rejected on the same rationale as the rejection as the rejection of **claims 11, 15, and 21**.

5. **Claims 4 and 5** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al** in view of US Patent 5,081,679 to **Dent** as applied to claim 1 above and further in view of US Patent Publication US 2002/0031126 to **Crichton et al.**.

5.1 **As per claims 4 and 5, Klingler et al.** substantially teaches forwarding/receiving encrypted packets from a local to a remote end, for example (see page 10, claims 18-21). **Klingler et al.** does not explicitly teach using a gateway controller, which is well known in the art of Internet Protocol network for connecting different protocol networks. However, **Crichton et al.** in an analogous art teaches a system for bit synchronous network communications over packet networks including Internet protocol network using gateways in an end-to-end communication path to perform analog to digital conversion and to communicate with packet network in a manner known in the art, for example (see page 5, paragraphs 0042 and 0047; see also background). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combined above to provide a gateway

controller as taught by **Crichton et al.** for forwarding and receiving encrypted packets through an Internet protocol to perform analog to digital conversion and to communicate with packet network in a manner known in the art. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Crichton et al.** so as to perform analog to digital conversion and to communicate with packet network in a manner known in the art.

6. **Claims 17 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US 2003/0003896 to **Klingler et al.** in view of US Patent Publication US 2002/0031126 to **Crichton et al.** and in view of US Patent 5,081,679 to **Dent**.

6.1 **Claim 17** contains some of the limitations of claims 6 and 13 except for sending encrypted data to a gateway, which was discussed in claims 4 and 5 above. Claim 17 also adds generating a second Real Time Protocol key stream for encrypting the voice packets in response to a collision detection wherein the multimedia terminal adapters have the same source identifier. **Dent** discloses the generation of new key when there is no synchronization, which may occur by handoff or resynchronization as discussed in claims 11, 15, and 21. Therefore claim 17 is rejected on the same rationale as the rejection of claims 4-6 and rejection of claims 11, 15, and 21.

Claim 18 is similar to the rejected **claims 12, 16, and 22**. Therefore, **claim 18** is rejected on the same rationale as the rejection of **claims 12, 16, and 22**.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin
Patent Examiner
April 14, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100